IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION

IN RE: BLACKBAUD, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 3:20-mn-02972-JMC MDL No. 2972

MEMORANDUM OF LAW IN SUPPORT OF BLACKBAUD'S MOTION TO DISMISS THE CONSOLIDATED COMPLAINT'S STATUTORY CLAIMS FOR FAILURE TO STATE A CLAIM PURSUANT TO FED. R. CIV. P. 12(B)(6)

TROUTMAN PEPPER HAMILTON SANDERS LLP
Ronald I. Raether, Jr.
5 Park Plaza, Suite 1400
Irvine, CA 02614
Telephone: (949) 622-2722
Facsimile: (949) 622-2239
ron.raether@troutman.com

Amy P. Williams
Joshua D. Davey
301 South College Street
Suite 3400
Charlotte, NC 28202
Telephone: (704) 998-4102
Facsimile: (704) 998-4051
amy.williams@troutman.com
joshua.davey@troutman.com

David N. Anthony
Ashley L. Taylor, Jr.
Timothy J. St. George
1001 Haxall Point, Suite 1500
Richmond, VA 23219
Telephone: (804) 697-5410
Facsimile: (804) 698-5118
david.anthony@troutman.com
ashley.taylor@troutman.com
timothy.st.george@troutman.com

BURR & FORMAN LLP
Celeste T. Jones
Post Office Box 11390
Columbia, SC 29211
Telephone: (803) 799-9800
Facsimile: (803) 753-3278
ctjones@burr.com

DUFFY & YOUNG, LLP
J. Rutledge Young, III
96 Broad Street
Charleston, SC 29401
Telephone: (843) 720-2044
Facsimile: (843) 720-2047
ryoung@duffyandyoung.com

Angelo A. Stio III
301 Carnegie Center
Suite 400
Princeton, NJ 08543
Telephone: (609) 951-4125
Facsimile: (609) 452-1147
angelo.stio@troutman.com

Cindy D. Hanson
600 Peachtree Street NE
Suite 3000
Atlanta, GA 30308
Telephone: (404) 885-3830
Facsimile: (404) 885-3900
cindy.hanson@troutman.com

Tambry L. Bradford
350 S. Grand Avenue, Suite 3400
Los Angeles, CA 90071
Telephone: (213) 928-9805
Facsimile: (213) 928-9850
tambry.bradford@troutman.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

FEDERAL CASES

STATE STATUTES

STATE RULES

Pursuant to Fed. R. Civ. P. 12(b)(6) and Case Management Order No. 7C (Dkt. 78), defendant Blackbaud, Inc. ("Blackbaud") submits this memorandum of law in support of its motion to dismiss Claims 15, 16, 24, 65, 67, 75, and 79 (the "Statutory Claims") of Plaintiffs' Consolidated Class Action Complaint (the "Complaint") for failure to state a claim upon which relief may be granted.

INTRODUCTION

Blackbaud offers cloud computing software that helps non-profit healthcare, educational, and charitable institution clients manage various forms of data for their constituents and donors. In May 2020, Blackbaud discovered that a ransomware attacker attempted to access, encrypt, and remove some of this third-party data. Upon discovery Blackbaud responded swiftly to successfully expel the third party from its environment, prevent encryption from occurring, and it negotiated the destruction of any data the third party may have accessed. After these efforts to contain and expel, Blackbaud alerted its clients of the ransomware attack (the "Ransomware Attack").

Plaintiffs—who *are not* Blackbaud *clients* but instead are donors and constituents of these clients—try to find fault in how Blackbaud handled the Ransomware Attack. As part of its efforts, Plaintiffs seek to improperly affix liability based on a host of state statutes that are simply inapplicable here, because the statutes either fail to apply to entities like Blackbaud or they fail to provide a remedy for the alleged harms Plaintiffs contend they sustained.

All of the Statutory Claims fail as a matter of law. The claims asserted under the California statutes (California Consumer Privacy Act ("CCPA") and the Confidential Medical Information Act ("CMIA")) fail to state a claim entirely. The CCPA imposes duties only on a "business," which the statute defines as a for-profit organization that collects California consumers' personal information. The CCPA does not impose those same duties upon "service providers," like Blackbaud, who "process[ ] information on behalf of a business."

The CMIA claim fares no better. Relevant here, the CMIA precludes "provider[s] of healthcare" from disclosing "medical information." But Blackbaud is not a "provider of healthcare" and the California Plaintiffs' "medical information" was not disclosed.

The Florida Plaintiffs claim Blackbaud violated the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), but that claim fails due to the absence of causation and damages. The Florida Plaintiffs allege only that they experienced some burden of additional phone calls "following" and "subsequent to" the Ransomware Attack, but temporal proximity is not sufficient to establish causation, especially given the additional weaknesses in Florida Plaintiffs' claims. Furthermore, the FDUTPA does not apply because the only harm the Florida Plaintiffs allege they suffered is not the direct, pecuniary loss needed to assert a cognizable FDUTPA claim.

The New Jersey Plaintiffs, like their contemporaries from California and Florida, disregard the essential elements of their New Jersey Consumer Fraud Act ("NJCFA") claim and therefore their claim fails for two independent reasons. First, Blackbaud's cloud-based software services and solutions are not "merchandise or real estate" sales "offered directly or indirectly to the public" covered by the Act. Second, their allegations of lost time, emotional distress, diminution in value of personal information, violation of privacy rights, and future, anticipated losses, do not constitute the types of "ascertainable losses" required to sustain a claim under the NJCFA.

The New York Plaintiffs allege a lackluster claim under New York General Business Law Section 349 ("GBL §349"), which only applies to "consumer-oriented" business practices. Here, however, it is undisputed that Blackbaud does not market its services to the consuming public at-large, meaning that GBL§349 does not apply.

The lone Pennsylvania Plaintiff has no basis to assert a claim under the Pennsylvania Unfair Trade Practices and Consumer Protection Law ("UTPCPL") because that law only protects

"purchasers" from their economic dealings with a business. Here, the Pennsylvania Plaintiff had no direct dealings with Blackbaud (let alone purchases), so this claim fails. Moreover, the UTPCPL claim lacks merit because the Pennsylvania Plaintiff alleges harm that is not covered by the law and not caused by any reliance on Blackbaud's conduct.

Finally, the South Carolina Plaintiffs cannot assert a claim under the South Carolina Data Breach Act (the "SCDBA"). The SCDBA applies only to persons "owning or licensing" data, which is not Blackbaud but instead Blackbaud's clients. Moreover, the SCDBA is inapplicable as it only applies to breaches of *specific* forms of data, none of which was involved in the Ransomware Attack.

For these reasons, and the analysis set forth below, the Court should dismiss the Statutory Claims—Counts 15, 16, 24, 65, 67, 75, and 79—of the Complaint.

I. BACKGROUND AND NATURE OF THE CASE

A. The Parties

According to the Complaint, Blackbaud is a company that "manages, maintains, and provides cloud computing software, services, and cybersecurity for clients including healthcare organizations, education institutions, and other non-profit corporations." Compl. ¶ 419.

The Plaintiffs who assert the Statutory Claims are students and donors of education institutions, patients and donors to healthcare organizations, and congregants of religious entities. *Id.* ¶¶ 4, 556. No Plaintiff is alleged to have purchased any product from Blackbaud, let alone a product for personal, family or household use. Indeed, none of the Plaintiffs are Blackbaud customers; instead, they are donors or constituents of Blackbaud's clients. *Id.* ¶ 12.

1. California Plaintiffs

Plaintiffs Kassandra Clayton, Philip Eisen, Mamie Estes, and Shawn Regan (collectively the "California Plaintiffs") allege that they are California residents and assert claims against

Blackbaud under the CCPA, Cal. Civ. Code § 1798.100, *et seq.*, and the CMIA, Cal. Civ. Code § 56, *et seq.*

Clayton alleges that she provided her information to Community Medical Centers and Trinity Health, both Blackbaud customers, in order to receive healthcare services. Compl. ¶ 52. She contends further that Community Medical Centers informed her that her "name, address, phone number, email address, date of birth, room number, patient identification number, name of hospital where treated, and the applicable hospital department or unit" were implicated in the Ransomware Attack. *Id.* She also claims she received notice from Trinity Health that her "name, address, phone number, email, most recent donation date, date of birth, age, inpatient/outpatient status, dates of service, hospital location, patient room number and physician name" were implicated in the Ransomware Attack. *Id.* She claims damages from the Ransomware Attack in the form of increased emails and calls, time spent and services purchased related to credit monitoring, emotional distress, losing the value of her personal information. *Id.* ¶¶ 55-57.

Eisen claims he provided his data to nonprofit Planned Parenthood to make a donation. *Id.* ¶¶ 62-63. Eisen received notice from Planned Parenthood "[i]n or around July 2020" that his information, including "street addresses and telephone numbers" was involved in the Ransomware Attack. *Id.* ¶ 63. Eisen claims he received notification that his information was found on the dark web and alleges he has seen a significantly increased amount of suspicious, unsolicited phishing telephone calls, text messages, and/or emails. *Id.* ¶ 69. Eisen also claims that he suffered damages in the form of time spent credit monitoring, emotional distress, and damage to value of his personal information. *Id.* ¶¶ 66-68, 70.

Plaintiffs Mamie Estes and Shawn Regan claim that nonprofit Crystal Stairs, Inc. notified them that their "name, [Social Security number "SSN"], and/or tax identification number" was

involved with the Ransomware Attack. *Id.* ¶¶ 72, 82. Estes claims that, over the past year, she received notices from her credit monitoring services that people are attempting to access her account on Amazon, PayPal, Apple, and Wells Fargo regarding fraudulent bank accounts and an increase in spam calls and has spent time dealing with these incidents as well. *Id.* ¶¶ 78-79. Estes also alleges that she suffered emotional distress and damage to the "value" of her personal information. *Id.* ¶¶ 76-77. Regan alleges she has experienced an unauthorized charge on her bank account, an increased number of "phishing and spam emails," emotional distress and a loss of value of her privacy. *Id.* ¶¶ 88-89.

2. Florida Plaintiffs

Plaintiffs William Carpenella and Dorothy Kamm allege that they are Florida residents and assert a claim against Blackbaud under the FDUTPA, Fla. Stat. § 501.201, *et seq*.

Carpenella claims that Stetson University notified him that his "name, SSN, date of birth, Student ID, demographic information, and philanthropic giving history, such as donation dates and amount," was involved in the Ransomware Attack. Compl. ¶ 103. Carpenella also claims that since last year, he received notification that his information was found on the dark web and he has seen an increase in spam telephone calls and has spent time dealing with these incidents as well. *Id.* ¶¶ 104, 108-09. He alleges that he has suffered emotional distress, violation of his privacy rights, and damage to the value of his personal information. *Id.* ¶ 106-07.

Kamm alleges that she provided her information to a variety of nonprofits including the Cornell Lab of Ornithology, Archbold Biological Station, and Planned Parenthood, to make donations, as well as to Barnes & Noble to sign up for its rewards program. *Id.* ¶ 112. While the Complaint asserts that Kamm's information was exposed and/or compromised, there is no detail as to what private information specifically was at issue in the Ransomware Attack. The Complaint further acknowledges that these organizations implicated by Kamm informed her that the credit

card numbers, bank account numbers, Social Security numbers, and additional categories data they provided to Blackbaud were encrypted. *Id.* ¶¶ 111-13. Nevertheless, she claims damages from the Ransomware Attack in the form of an increase in unsolicited calls, text, or emails, time spent monitoring and dealing with these incidents, emotional distress, violation of her privacy rights, and damage to the "value" of her personal information. *Id.* ¶¶ 114-18.

3. New Jersey Plaintiffs

Plaintiffs Martin Roth and Rachel Roth allege that they are residents and citizens of New Jersey and New York, respectively, and assert a claim against Blackbaud under the NJCFA, N.J. Stat. Ann. § 56:8-1, *et seq*.

Both New Jersey Plaintiffs claim that Joseph Kushner Hebrew Academy notified them, "[i]n or around August 2020," that their "name[s], address[es], date[s] of birth and giving histor[ies]" may have been involved with the Ransomware Attack. Compl. ¶¶ 229, 239. Later, on November 23, 2020, the New Jersey Plaintiffs allege that they received additional notice from Joseph Kushner Hebrew Academy, explaining that legacy software was not encrypted and "may have contained [Rachel] Roth's SSN" or other information. *Id.* ¶¶ 230, 240.

The New Jersey Plaintiffs allege that Blackbaud offered them credit monitoring services, which they declined. *Id.* ¶¶ 233, 243. Martin Roth claims that he experienced numerous unauthorized credit card purchases and a lowered credit score. *Id.* ¶ 236. Rachel Roth has alleged that she received an alert from Capital One indicating that her information was found on the dark web. *Id.* ¶ 245. They claim to have collectively spent 25 hours to date on monitoring their credit and both allege that they have suffered emotional distress, violation of their privacy rights, and damage to the "value" of their personal information. *Id.* ¶¶ 232, 234-35, 241-42, 244.

4. New York Plaintiffs

Plaintiffs Ralph Peragine and Karen Zielinski allege that they are residents and citizen of New York and seek to assert a claim against Blackbaud under GBL §349, N.Y. Gen. Bus. Law § 349, *et seq*.

Peragine alleges that he provided personal and health-related information to New Haven Hospital to receive healthcare services. Compl. ¶ 249. He further contends that New Haven Hospital notified him that his "name, address, phone number, date of birth, philanthropic history, name of doctor and dates of service at the hospital," were involved in the Ransomware Attack. *Id.* ¶ 250. Peragine claims to have spent 3 hours to date monitoring his credit. *Id.* ¶ 252. He claims that someone applied for and received unemployment benefits in his name, and that he has spent time dealing with this and credit monitoring. *Id.* ¶ 256. He alleges that he suffered emotional distress and damage to the value of his personal information. *Id.* ¶¶ 254-55.

Zielinski provided information to Roswell Park Alliance Foundation and Life of Light Rescue Mission to make charitable donations. *Id.* ¶¶ 258-59. She claims that she received notice from Roswell Park Alliance Foundation that her "contact information, date of birth, limited demographic data and a history of her relationship with the Alliance Foundation such as donation dates and amounts" were compromised. *Id.* ¶ 260. Additionally, while the Complaint alleges that Zielinski received notice from Light of Life Rescue Mission, the Complaint does not include specifics on which types of information were allegedly impacted by the Ransomware Attack, except to note that he was informed that it "did not involve the exposure of usernames, passwords, credit card information, bank account information, or SSNs" for the Roswell Park Alliance Foundation. *Id.* ¶ 261. Finally, Zielinski claims damages from the Ransomware Attack in the form of increased emails or calls, time spent monitoring her accounts, emotional distress, and damage to the "value" of her personal information. *Id.* ¶¶ 264-66.

5. Pennsylvania Plaintiff

Plaintiff Christina Duranko alleges that she is a resident and citizen of Pennsylvania and seeks to assert a claim against Blackbaud under the UTPCPL, 73 Pa. Stat. § 201-1, *et seq*.

Duranko claims that she provided her health and personal information to Allegheny Health Network ("AHN") to receive healthcare services. Compl. ¶¶ 310-11. AHN notified Duranko "[i]n or around December 4, 2020" that her "name, date of birth, address, business address, phone numbers, email addresses, and limited medical information, such as dates she may have had services provided at AHN, her treating provider's name, and the AHN location" may have been accessed by the attacker. *Id.* ¶ 311. As damages, Duranko alleges that she has spent time monitoring her accounts, that she has suffered emotional distress, a violation of her privacy rights, and damage to the "value" of her personal information. *Id.* ¶¶ 313, 315-16.

6. South Carolina Plaintiffs

Plaintiffs Latricia Ford and Clifford Scott allege that they are citizens and residents of South Carolina (collectively "South Carolina Plaintiffs") and seek to assert a claim against Blackbaud under the South Carolina Data Breach Security Act ("SCDBA"), S.C. Code § 39-1-90, *et seq*.

Ford claims that she provided personal and health-related information to her provider Roper St. Francis Hospital to receive healthcare services. Compl. ¶¶ 321-22. She contends further that Roper St. Francis Hospital informed her "[i]n or around September 2020" that her "name, gender, date of birth, address, date(s) of treatment, department(s) of service, and treating physician(s)" were involved in the Ransomware Attack. *Id.* ¶¶ 322-23. She claims an increase in suspicious emails and phone calls, received numerous cyber alerts indicating that individuals have knowledge of her name, email, previous home address, and telephone number, and has been notified that someone requested a fraudulent insurance quote, resulting in a soft inquiry on her

credit. *Id.* ¶ 328. She alleges someone called her impersonating her internet provider in attempt to gain access to her work computer. *Id.* She also claims that she has suffered emotional distress and damage to the "value" of her personal information. *Id.* ¶¶ 326-27.

Scott alleges that he provided his personally identifying information to the University of South Carolina to make charitable donations. *Id.* ¶¶ 332-33. He further alleges that the University of South Carolina informed him "[i]n or around September 2020" that his "name, contact information, demographic information, date of birth and giving profiles and history" were compromised. *Id.* ¶ 333. Finally, Scott claims damages from the Ransomware Attack in the form of increased emails and calls, time spent monitoring his accounts, emotional distress, and damage to the "value" of his personal information. *Id.* ¶¶ 334, 336-38.

B. The Ransomware Attack

In May 2020, Blackbaud discovered that it was the victim of the Ransomware Attack, which was orchestrated by a threat actor who hacked into Blackbaud's systems and demanded payment to delete data that the threat actor stole from Blackbaud. *Id.* ¶ 1. After discovering the Ransomware Attack, Blackbaud worked with forensic experts such as Kudelski Security, and with law enforcement to successfully expel the threat actor from its systems. *Id.* ¶¶ 499, 549-50. After expulsion of the threat actor and an initial determination was made concerning the scope of the information involved, Blackbaud provided its customers with notice of the Ransomware Attack. *Id.* ¶¶ 497-99. After further forensic investigation, Blackbaud sent out a second notice to a limited number of its clients that the "'cybercriminal may have accessed some unencrypted fields intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords.'" *Id.* ¶ 26.

LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the Complaint. *ACA Fin. Guar. Corp. v. City of Buena Vista, Va.*, 917 F.3d 206, 211 (4th Cir. 2019). Under that Rule, the Court—after accepting all well-pleaded factual allegations as true but giving no such deference to legal assertions, *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)—should dismiss a Complaint that "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). The claim for relief must be "plausible," rising "above the speculative level." *Walters v. McMahen*, 684 F.3d 435, 439 (4th Cir. 2012) (citation omitted). "Labels, conclusions, recitation of a claim's elements, and naked assertions devoid of further factual enhancement will not suffice" to overcome a Rule 12(b)(6) motion. *ACA Fin. Guar. Corp.*, 917 F.3d at 211.

ARGUMENT

I. THE CONSOLIDATED COMPLAINT DOES NOT STATE A CLAIM UNDER THE CALIFORNIA CONSUMER PRIVACY ACT (CLAIM 15).

California Plaintiffs' CCPA claim fails as a matter of law because there is no allegation that Blackbaud is a regulated "business" under the Act. Instead, it is a service provider to its business customers, meaning that the CCPA provisions Plaintiffs invoke have no application to Blackbaud. Therefore, the CCPA claim must be dismissed.

1. The California CCPA Only Applies To Regulated "Business[es]," With No Similar Duties Imposed Upon Mere "Service Providers."

The California Plaintiffs have attempted to plead a claim under § 1798.150(a)(1) of the CCPA, which provides that "[a]ny consumer whose nonencrypted or nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action . . . ." Cal. Civ. Code § 1798.150(a)(1). As California Plaintiffs

acknowledge, Compl. ¶¶ 821-22, their CCPA claim depends on establishing that Blackbaud is a "business" as defined by the CCPA, *Bahari v. State Bar of Cal.*, No. 19CV360452, 2020 WL 5493870, at *3 (Cal. Super. Aug. 6, 2020). Pursuant to California Civil Code § 1798.140(c), a "business" is any organization that, among other requirements, "operate[s] for the profit or financial benefit of its shareholders or other owners," (b) "collects consumers' personal information," and (c) either "alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information." Cal. Civ. Code § 1798.140(c)(1)(A)–(C).

While the CCPA directly imposes obligations on regulated "businesses," the CCPA also recognizes the limited role of "service providers" like Blackbaud. Pursuant to California Civil Code § 1798.140(v), a "service provider" is any (1) for-profit entity that (2) "processes information on behalf of a business," which (3) receives a consumer's personal information for a business purpose, (4) "pursuant to a written contract," which "prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business." Cal. Civ. Code § 1798.140(v).

Importantly, the CCPA imposes no affirmative obligations on "service providers," as opposed to "businesses." *See, e.g.*, Cal. Civ. Code § 1798.100(b) ("A ***business*** that collects a consumer's personal information shall . . . inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used." (emphasis added)); Cal. Civ. Code § 1798.110(c) ("A ***business*** that collects personal information about consumers shall disclose . . . the categories of personal information it has collected about consumers . . . ." (emphasis added)). And, most importantly here, Section 1798.150, the provision under which Plaintiffs bring this claim, Compl. ¶ 825, offers to

"consumer[s] whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the ***business's*** violation of the duty to implement and maintain reasonable security procedures and practices" the right to "institute a civil action." Cal. Civ. Code § 1798.150(a)(1) (emphasis added).

Thus, the plain text of the CCPA imposes specific duties only on "business[es]" that collect personal information, not on "service providers" like Blackbaud with whom those businesses contract for data processing.

2. Blackbaud Is A "Service Provider" Under The CCPA, Meaning That Plaintiffs Cannot State A Claim.

In the Complaint, California Plaintiffs make one conclusory allegation that Blackbaud is a "***business*** that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e)." Compl. ¶ 822 (emphasis added). However, the Complaint is devoid of any facts suggesting a plausible basis to claim Blackbaud qualifies as a regulated "business" under the statute. Instead, the factual allegations in the Complaint demonstrate Blackbaud's status as a service provider that is not subject to a CCPA action.

As Plaintiffs allege, Blackbaud only "obtains, receives, or accesses consumers' personal information ***when customers use Blackbaud's products*** to maintain and process consumer data." *Id.* (emphasis added). In that capacity, Blackbaud contracted with clients to provide software as a service platform to maintain and process data collected and disclosed by its clients, *see, e.g., id.* ¶¶ 419, 822, thereby acting only as a "legal entity . . . that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract," Cal. Civ. Code § 1798.140(v). Put another way, Plaintiffs' allegations confirm that Blackbaud is a service provider under § 1798.140(v). But the CCPA does not impose those same duties upon "[s]ervice provider[s]" as it does on "businesses," including

under § 1798.150 of the California Civil Code, the provision under which Plaintiffs bring their claims. *See* Compl. ¶ 825. Because Blackbaud acted only as a service provider, the CCPA imposes no obligations on Blackbaud and therefore any claim premised on a violation of the CCPA fails. *See* Cal. Civ. Code § 1798.150(a)(1).

Furthermore, some of the California Plaintiffs' allegations relate only to Blackbaud's services offered to non-profit entities that are *themselves* not covered by the CCPA, and thus these Plaintiffs' claims are even further removed from the CCPA's scope. This is the case because regulated "business[es]" under the CCPA encompass only those entities "organized or operated for the profit or financial benefit of its shareholders or other owners." Cal. Civ. Code § 1798.140(c)(1).

Here, California Plaintiffs Eisen, Estes, and Regan all allege that they provided their information to Planned Parenthood and Crystal Stairs, Inc., which are both non-profit entities. Compl. ¶¶ 62–63, 72, 82.[1] Therefore, Plaintiffs Eisen, Estes, and Regan could not even maintain a claim against these nonprofit entities that actually collected their information, *see* Cal. Civ. Code § 1798.150 ("civil action" available only against a "business[ ]"); *id.* § 1798.140(c)(1) (defining "business" only to include an "entity organized or operated for . . . profit"), so derivative liability against Blackbaud, acting as a mere "service provider" to these entities, is similarly precluded by the CCPA.

[1] California Planned Parenthood Education Fund, Inc., IRS Form 990 (2019), *available at* https://apps.irs.gov/pub/epostcard/cor/680358026_201906_990_2021020917698478.pdf; Planned Parenthood Action Fund, Inc., IRS Form 990 (2019), *available at* https://apps.irs.gov/pub/epostcard/cor/133539048_201906_990O_2020100217347215.pdf; Crystal Stairs, Inc., IRS Form 990T (2020), *available at* https://apps.irs.gov/pub/epostcard/cor/953510046_202006_990T_2020121517478768.pdf. This Court may take judicial notice of these public records without converting Blackbaud's Rule 12(b)(6) motion into one for summary judgment. *Philips v. Pitt Cty. Mem. Hosp.*, 572 F.3d 176, 180 (4th Cir. 2009).

II. THE COMPLAINT DOES NOT STATE A CLAIM UNDER THE CALIFORNIA CMIA (CLAIM 16).

The California CMIA provides a claim against "[a] provider of health care, health care service plan, or contractor . . . [for] disclos[ing] medical information regarding a patient . . . without first obtaining an authorization." Cal. Civ. Code § 56.10(a); *see also id.* § 56.101 (duty to maintain medical information against same groups).

By its express terms the CMIA only applies to a "provider of health care, health care service plan, or contractor." Cal. Civ. Code § 56.10(a). Plaintiffs "naked[ly] assert[ ]," *ACA Fin. Guar. Corp.*, 917 F.3d at 211, that Blackbaud meets the definition of a "provider of healthcare" under the CMIA. Compl. ¶ 838. The Court should not credit that allegation, however, because it contravenes the CMIA's definition of "provider of health care," which the CMIA defines in two ways. First, that term includes "any clinic, health dispensary, or health facility licensed pursuant to [California law]." Cal. Civ. Code § 56.05(m). This definition plainly does not apply to Blackbaud. Second, the term includes "[a]ny business that offers software or hardware ***to consumers*** . . . designed to maintain medical information, . . . in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual." *Id.* § 56.06(b) (emphasis added). It is the latter provision that the California Plaintiffs invoke here. Compl. ¶ 838. But this latter definition does not apply, for three reasons: first, because the information at issue is not "medical information," second, because Blackbaud is not a "provider of health care" under the CMIA as it offered no services to the Plaintiffs, and third, because Plaintiffs do not allege that Blackbaud maintained their information "for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition."

First, Plaintiffs' personal information that was supposedly viewed by an unauthorized party does not meet the CMIA's statutory definition of "medical information." Cal. Civ. Code § 56.05(j). The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." *Id.* California courts have interpreted this definition of "medical information" as requiring not "just any patient-related information held by a health care provider," but rather "'individually identifiable information' [that] also include[s] 'a patient's medical history, mental or physical condition, or treatment.'" *Eisenhower Med. Ctr. v. Superior Court*, 226 Cal. App. 4th 430, 435 (Cal. Ct. App. 2014). Thus, "demographic or numeric information that does not reveal medical history, diagnosis, or care," such as a "person's name, medical record number (MRN), age, date of birth, and last four digits of the person's Social Security number" *does not* constitute "medical information" under the CMIA. *Id.* at 432, 435.

The information allegedly compromised for Eisen included only "street addresses and telephone numbers." Compl. ¶ 63. Plaintiffs Estes and Regan allege that the supposedly compromised data was their "name, SSN, and/or tax identification number." *Id.* ¶¶ 72, 82. As explained in *Eisenhower*, however, this information plainly does not meet the CMIA's definition of "medical information" because it does not reveal anything about these California Plaintiffs' "medical history, diagnosis, or care." 226 Cal. App. 4th at 435.

Clayton contends that her allegedly compromised personal information may have included her "patient identification number, name of hospital where treated, applicable hospital department or unit" as well as "inpatient/outpatient status, dates of service, hospital location, patient room number and physician name." Compl. ¶ 52. However, that information also is not "medical

information," as defined by the CMIA, because that "definition does not encompass demographic or numeric information that ***does not reveal medical history, diagnosis, or care***." *Eisenhower*, 226 Cal. App. 4th at 435 (emphasis added). That information does not provide any insight regarding Clayton's medical history, mental condition or treatment, and instead shows only "the mere fact that a person may have been a patient at the hospital at some time," which the California courts have concluded "is not sufficient" under the CMIA, and, indeed, is near-identical to the forms of information the *Eisenhower* court found to be *outside* the scope of statutory term "medical information." *Id.* at 435, 436–37. Thus, even if the Ransomware Attack resulted in unauthorized third parties viewing California Plaintiffs' personal information as alleged, the California Plaintiffs cannot state a claim for relief under the CMIA. *Id.* at 437.

Second, Blackbaud does not meet the statutory definitions of the entities that are subject to the CMIA. The California Plaintiffs allege that Blackbaud is a "provider of health care" under § 56.06(b), Compl. ¶ 838, which includes only "business[es] that offer[ ] software or hardware to consumers" for certain covered purposes Cal. Civ. Code § 56.06(b). But California Plaintiffs never had direct contact with Blackbaud and at no point purchased a product from Blackbaud. *See* Compl. ¶ 12. In fact, the California Plaintiffs concede that Blackbaud is a provider of "cloud computing software, services, and cybersecurity for clients," which are "healthcare organizations, education institutions, and other non-profit corporations," Compl. ¶ 419, i.e., businesses, *not* consumers. And Plaintiffs nowhere allege that Blackbaud offered its software or hardware to them, *or any other consumer*. By Plaintiffs' own allegations, then, Blackbaud has not "offer[ed] software or hardware *to consumers*," Cal Civ. Code § 56.06(b) (emphasis added), and does not meet the statutory definition of a "provider of healthcare" as necessary for liability under the CMIA.

Third, California Plaintiffs fail to allege that Blackbaud collected their information "for purposes of allowing the individual to manage his or her information, or for the diagnosis, treatment, or management of a medical condition of the individual." Cal. Civ. Code § 56.06(b). The California courts interpret the CMIA according to the "plain meaning of the [statutory] language." *Regents of Univ. of Cal. v. Superior Court*, 220 Cal. App. 4th 549, 558 (Cal. Ct. App. 2013). This "purposes" requirement, set off from the remainder of the subsection by commas, applies to the entirety of this definition of "provider of health care." *See White v. Cty. of Sacramento*, 646 P.2d 191, 193 (Cal. 1982). Therefore, Blackbaud would only qualify as a "provider of healthcare" under § 56.06(b), for purposes of this motion, if Plaintiffs alleged that its services are intended to "allow[ ] [Plaintiffs] to manage his or her information" or for medical diagnosis, treatment, or management. No California Plaintiff sufficiently alleges this requirement.

Plaintiffs Eisen, Regan, and Estes, allege only they were "required to provide [their personal information] to entities to whom [they] regularly made charitable donations." Compl. ¶ 62; *see id.* at ¶¶ 71, 81 (similar). None alleges that they had any ability to later access and manage this information they provided to these "Social Good Entities." And none alleges that they provided such information for any medical purpose, let alone for the "diagnosis, treatment, or management of a medical condition," Cal. Civ. Code § 56.06(b), sufficient to raise a claim under the CMIA. *See* Compl. ¶¶ 62, 71, 81. Clayton's claims, although *somewhat* related to medical services, fail for the same reasons. Clayton alleges only that she "was required to provide her [personal health information] to several healthcare providers *as a predicate to receiving healthcare services*." Compl. ¶ 52 (emphasis added). But she does not contend that any information she provided was "for the diagnosis, treatment, or management of a medical condition," § 56.06(b), rather than mere boilerplate information for healthcare-provider admissions *see* Compl. ¶ 52

(noting that her information allegedly accessed related only to "her name, address, phone number, email address, date of birth, room number, patient identification number, name of hospital where treated, [and] applicable hospital department or unit."). And she nowhere alleges that she had any further involvement with her information, such that she could "manage" it. *Id.* Therefore, no California Plaintiff at all alleges that Blackbaud maintained their information for the specific "purposes" required under the statute, so this is another, independent basis to dismiss the CMIA claims.

III. THE COMPLAINT DOES NOT STATE A CLAIM UNDER THE FDUTPA (CLAIM 24).

The Florida Plaintiffs attempt to assert a claim under the FDUTPA based on various iterations of the allegation that Blackbaud failed to implement and maintain reasonable security measures. Compl. ¶ 933. To state a claim for damages under FDUTPA, a plaintiff must allege: "(1) a deceptive act or unfair practice; (2) causation; and (3) actual damages." *City First Mortg. Corp. v. Barton*, 988 So.2d 82, 86 (Fla. Dist. Ct. App. 2008) (citation omitted). Here, the Florida Plaintiffs fail to allege causation beyond mere temporal proximity, and they also fail to allege any actual damages to support a FDUTPA claim. Additionally, the Florida Plaintiffs' claim for injunctive relief must be dismissed because there is no plausible threat of future harm based on the alleged FDUTPA violation, as required for such relief.

A. The Florida Plaintiffs Fail To Allege Necessary Causation Under FDUTPA.

Under Florida law, "temporal proximity alone does not establish causation." *Cerna v. Bioavailability Clinic*, 815 So. 2d 652, 656 (Fla. Dist. Ct. App. 2002); *cf. Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1327 (11th Cir. 2012). Nevertheless, the Complaint relies only on the timing of claims of identity theft and phishing schemes "subsequent" to the Ransomware Attack to try to tie them causally. Compl. ¶¶ 108, 117. Indeed, the Florida Plaintiffs' own allegations belie the

plausibility of such claims of causation. Carpenella, for instance, alleges only an "increase in the number of spam phone calls" and notifications "following" the Ransomware Attack, *id.* ¶ 108, but the information involved in the Ransomware Attack *did not* include his phone number, *id.* ¶ 103. Kamm's causation allegations are, remarkably, even weaker. While she claims she experienced "increased" telephone calls "subsequent to" the Ransomware Attack, *id.* ¶ 117, her allegations confirm that any personal information about her implicated by the Ransomware Attack was encrypted. *Id.* ¶¶ 112-13. Thus, the Florida Plaintiffs have failed to allege causation beyond temporal proximity, which is insufficient as a matter of law.

B. The Florida Plaintiffs Did Not Suffer Actual Damages For Purposes Of The FDUPTA.

The Florida Plaintiffs also have not adequately alleged the element of actual damages for their FDUTPA claim because they have only described consequential, rather than actual, damages.

Actual damages, "the third element of a FDUTPA claim" is a "'term of art' defined by 'the difference in the market value of the product or service in the condition in which it was delivered and its market value in the condition in which it should have been delivered.'" *Diversified Mgmt. Sols., Inc. v. Control Sys. Research, Inc.*, No. 15-81062, 2016 WL 4256916, at *5 (S.D. Fla. May 16, 2016) (quoting *Urling v. Helms Exterminators, Inc.*, 468 So. 2d 451, 454 (Fla. Dist. Ct. App. 1984)). Moreover, "nominal damages, speculative losses, or compensation for subjective feelings of disappointment are not recoverable under the FDUTPA . . . nor may a Plaintiff[s] recover 'consequential damages.'" *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 993 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014) (court interpreting Florida law). "Consequential damages" under Florida law are all those that "were not the direct or necessary consequence of" the

defendant's conduct. *Keystone Airpark Auth. v. Pipeline Contractors, Inc.*, 266 So. 3d 1219, 1222–23 (Fla. Dist. Ct. App. 2019).

As an initial matter, the Florida Plaintiffs fail to allege actual identity theft or any pecuniary loss resulting from the breach. Plaintiffs Kamm and Carpenella do not allege that their identity was stolen or even that they were subject to fraudulent activity generally, but, rather, only that they have experienced "an increase in spam telephone calls" and for Carpenella, "notification that his information was found on the dark web," Compl. ¶¶ 108, 117, among various other concerns. But these allegations do not contend that Plaintiffs have experienced any pecuniary or physical loss, which dooms their claims. *See Himes v. Brown & Co. Secs. Corp.*, 518 So.2d 937, 938 (Fla. Dist. Ct. App. 1987) (affirming bench-trial judgment to defendant under FDUTPA for lack of damages where plaintiff sustained no out-of-pocket losses); *Macias v. HBC of Fla., Inc.*, 694 So.2d 88, 90 (Fla. Dist. Ct. App. 1997) (affirming dismissal for failure to state a claim for same reason).

Instead, the Florida Plaintiffs attempt to allege damages in several ways, none of which satisfy FDUTPA's damages element, claiming: (1) time/money spent on credit monitoring, Compl. ¶¶ 104, 109, 114; (2) emotional distress, *id.* ¶¶ 106, 115; (3) damage to the value of their personal information; (4) risk of future harm or identity theft; and (5) violation of privacy rights, *id.* ¶¶ 107, 116. Those allegations, however, all fail as a matter of law. That is true for several reasons.

First, time and money spent monitoring accounts in the wake of a disclosed data breach do not support a claim under FDUTPA, because they are merely consequential damages. *See, e.g.*, *In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2019 WL 3502993, at *6 (M.D. Fla. Aug. 1, 2019); *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 424 n. 33 (E.D. Va. 2020) ; *In re Brinker Data Incident Litig.*, No. 3:18-CV-686-J-32MCR, 2020 WL

691848, at *13 (M.D. Fla. Jan. 27, 2020) ("unauthorized charges, lost time, and lost cash-back rewards are all consequential damages"). Therefore, Plaintiffs claims premised on monitoring accounts are not compensable under this Act.

Second, "emotional distress" cannot support a FDUTPA claim. *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d at 993 ("[C]ompensation for subjective feelings of disappointment are not recoverable under the FDUTPA . . . .").

Third, courts have consistently rejected the claim that personal information has an independent value, such that its diminution could qualify as an actual injury under the FDUTPA. *See, e.g.*, *Burrows v. Purchasing Power, LLC*, No. 1:12–cv–22800, 2012 WL 9391827, at *3 (S.D. Fla. Oct. 18, 2012) ("Personal data does not have an apparent monetary value that fluctuates like the price of goods or services."); *see also Schauer v. Morse Operations, Inc.*, 5 So. 3d 2, 7 (Fla. Dist. Ct. App. 2009) ("[D]amages to [the plaintiff's] credit rating are consequential.").

Fourth, courts have routinely dismissed complaints based on the risk of future identity theft. *See, e.g.*, *Siever v. BWGaskets, Inc.*, 669 F. Supp. 2d 1286, 1294 (M.D. Fla. 2009) ("Under FDUTPA, 'actual damages' do not include consequential damages, precluding recovery of future lost profits.") (citations omitted).

Finally, a speculative claim of violation of "privacy rights" does not state a claim for actual damages under the FDUTPA, because it "does not provide for the recovery of nominal damages, speculative losses, or compensation for subjective feelings." *Barton*, 988 So. 2d at 86 (citation omitted). Such an esoteric claim plainly does not fit within the FDUTPA's limited scope of damages relating to "the difference in the market value of the product or service in the condition in which it was delivered and its market value in the condition in which it should have been delivered.'" *Urling*, 468 So. 2d at 454.

IV. THE COMPLAINT DOES NOT STATE A CLAIM UNDER THE NJCFA (CLAIM 65).

The NJCFA prohibits a person from using an "unconscionable commercial practice, deception, fraud," or the like "in connection with the sale or advertisement of any merchandise or real estate." N.J. Stat. Ann. § 56:8-2. An NJCFA claim has three requirements: (1) unlawful conduct by defendant that violates the NJCFA; (2) an ascertainable loss suffered by plaintiff; and (3) a causal relationship between the unlawful conduct and the ascertainable loss. *Bosland v. Warnock Dodge, Inc.*, 964 A.2d 741, 749 (N.J. 2009). Here, the NJCFA claim fails because Plaintiffs have not alleged conduct by Blackbaud that falls under the purview of the NJCFA, nor any ascertainable loss.

A. Blackbaud's Services Do Not Fall Within The Coverage Of The NJCFA, Which Only Applies To The Sale Of Merchandise.

As noted immediately above, the NJCFA prohibits fraud and other deceptive practice only "in connection with ***the sale or advertisement of any merchandise or real estate***." N.J. Stat. Ann. § 56:8-2 (emphasis added). The NJCFA defines merchandise as "any objects, wares, goods commodities, services or anything offered, directly or indirectly ***to the public for sale***." *Id.* § 56:8-1 (emphasis added).

"[T]he CFA 'is not intended to cover every transaction that occurs in the marketplace[,]' but, rather, '[i]ts applicability is limited to consumer transactions which are defined both by the status of the parties and the nature of the transaction itself.'" *Cetel v. Kirwan Fin. Grp., Inc.*, 460 F.3d 494, 514 (3d Cir. 2006) (quoting *Arc Networks, Inc. v. Gold Phone Card Co.*, 756 A.2d 636, 637 (N.J. Super. Ct. Law Div. 2000)). Accordingly, when a complex product is not being offered for sale to the general public, it does not give rise to a claim under the NJCFA. *Tremco Canada Div., RPM Canada v. Dartronics, Inc.*, No. CIV.A. 13-1641 SRC, 2013 WL 2444076, at *2–3 (D.N.J. June 4, 2013). To that end, courts have consistently held that a complex software contract

between sophisticated corporate entities is outside the purview of the NJCFA because a "heavily negotiated contract between two sophisticated corporate entities does not constitute a 'sale of merchandise' within the intent of the CFA." *Princeton Healthcare Sys. v. Netsmart N.Y., Inc.*, 29 A.3d 361, 365 (N.J. Super. Ct. App. Div. 2011). Similarly, the sale of services between a wholesaler and a manufacturer could not give rise to an NJCFA claim because "those services are not services sold to the general public and thus are not 'merchandise' under the NJCFA." *Bracco Diagnostics, Inc. v. Bergen Brunswig Drug Co.*, 226 F. Supp. 2d 557, 561 (D.N.J. 2002).

This case is similar to *Princeton and Bracco.* The Complaint alleges that Blackbaud provided bespoke and complex data security services to its clients, who were "Social Good Entities" and not the consuming public. *See* Compl. ¶¶ 430-41. Indeed, New Jersey Plaintiffs admit that "Blackbaud has professional and managed services in which its expert consultants provide data conversion, implementation, and customization services for each of its software solutions." *Id.* ¶ 436. Blackbaud's customers are not the New Jersey Plaintiffs or the public more generally, but rather are sophisticated businesses and entities. *See id.* ¶ 4 (Blackbaud markets its services to "Social Good Entities," not the consuming public); *id.*¶ 12 (Blackbaud identified its clients not as the general consuming public, but as "arts and cultural organizations, companies . . . , faith communities, foundations, healthcare organizations, higher education institutions, individual change agents, K-12 schools, and nonprofit organizations"); *id.* ¶ 35 (entities—not consumers—contracted with Blackbaud to host the data); *see also id.* ¶¶ 14, 15, 419.

Therefore, Blackbaud's sales all fall within the categories of "heavily negotiated contract[s] between two sophisticated corporate entities," *Princeton*, 29 A.3d at 365, not "sold to the general public," *Bracco*, 226 F. Supp. 2d at 561, that fall outside the NJCFA's purview.[2]

[2] Indeed, Plaintiff Rachel Roth does not allege she purchased *anything*, but rather appears to allege only that she "attended Joseph Kushner Hebrew Academy from approximately 2005 through 2014." Compl.

B. The New Jersey Plaintiffs Fail To Plead An "Ascertainable Loss."

The New Jersey Plaintiffs also fail to allege an "ascertainable loss" under the NJCFA, an essential element of their claim. *See* N.J. Stat. § 56:8-19 (limiting claims to a plaintiff "who suffers any ascertainable loss of moneys or property, real or personal"); *see generally Hinton v. Heartland Payment Sys., Inc.*, No. CIV. A. 09-594 MLC, 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009). An "ascertainable loss" "means that plaintiff must suffer a definite, certain and measurable loss, rather than one that is merely theoretical." *Bosland*, 964 A.2d at 749 (citing *Thiedemann v. Mercedes-Benz USA, LLC*, 872 A.2d 783, 792 (N.J. 2005)).

The New Jersey Plaintiffs allege that they have suffered: (1) lost time addressing the impacts of the Ransomware Attack (Compl. ¶¶ 232, 241); (2) emotional distress (*id.* ¶ 234, 242); (3) diminution in the value of their personal information (*id.* ¶¶ 235, 244); (4) violation of unspecified privacy rights (*id.* ¶¶ 235, 244); and (5) anticipated loss of time and money in the future addressing the Ransomware Attack or being subject to future identity theft (*id.* ¶¶ 235, 244). Each of these is plainly insufficient.

Lost personal time is not ascertainable loss. *See, e.g., Smith v. Trusted Universal Standards in Elec. Transactions, Inc.*, No. 09-4567 RBK KMW, 2011 WL 900096, at *14 (D.N.J. Mar. 15, 2011) (dismissing NJCFA claims where "[t]he only 'loss' Plaintiff alleges is the value of his personal time . . . 'conducting extensive troubleshooting to try to solve the problem and avoid future incidents.'").

Emotional distress is not recoverable under the NJCFA. *See, e.g., Tobing v. Parker McCay, P.A.*, No. 317CV00474, 2020 WL 7768410, at *7 (D.N.J. Dec. 30, 2020) ("It is well established

¶ 240. Having purchased nothing, the NJCFA is inapplicable. *Lawmen Supply Co. of N.J., Inc. v. Glock, Inc.*, 330 F. Supp. 3d 1020, 1044 (D.N.J. 2018) ("The NJCFA is intended to protect consumers who ***purchase*** goods or services generally sold to the public at large.") (emphasis added; citation omitted).

that damages for emotional distress alone are not recoverable as an ascertainable loss under the NJCFA." (quoting *Cole v. Laughrey Funeral Home*, 869 A.2d 457, 463 (N.J. Super. Ct. App. Div. 2005)).

The New Jersey Plaintiffs' alleged violations of their "privacy rights" and diminution of value for their personal information are bolstered by no facts about the change in value of that information and are therefore insufficiently specific to support a claim. *See, e.g.*, *Lieberson v. Johnson & Johnson Consumer Cos.*, 865 F. Supp. 2d 529, 541–42 (D.N.J. 2011). In any event, "intangible harm as a result of alleged invasions of their rights of privacy and confidentiality" of their personal information does not "support a private cause of action under the [NJ]CFA." *Castro v. NYT Television*, 851 A.2d 88, 96 (N.J. Super. Ct. App. Div. 2004).

Finally, vague and speculative anticipated harm—such as anticipated future loss of time—is not an ascertainable loss under the NJCFA. *Bosland*, 197 N.J. at 558 (theoretical loss is not recoverable under the NJCFA).

Apart from those insufficient allegations of harm, the New Jersey Plaintiffs also point to final, supposed "ascertainable losses" in the form of unauthorized credit card purchases on Plaintiff Martin Roth's credit card and a decline in his credit score. Compl. ¶ 236. Plaintiff Rachel Roth also alleges that she received "an alert on February 11, 2020 from Capital One that her information was found on the dark web," *id.* ¶ 245. Those claimed "losses" are, however, speculative and insufficient. Martin Roth does not allege that he actually incurred these unauthorized credit card charges or that any alleged charges were not reimbursed or deemed to not be his responsibility. He also fails to allege that his decreased credit score was the result of the Ransomware Attack; rather he contends they only happened subsequent to the Ransomware Attack. *Compare id.* ¶ 236 (noting only that identity theft happened "subsequent to" the Attack), *with id.* ¶ 237 (identifying

lost time "[a]s a result" of the Attack). At best, he is speculating that the credit score decrease happened as a result of the Ransomware Attack. And even that pure speculation is unwarranted, because he does not even allege his credit card information was breached. *Id.* ¶¶ 229-30. Such implausible inference falls well short of the NJCFA's requirement of the strong causal link or "direct correlation between the unlawful practice and the loss," *Heyert v. Taddese*, 70 A.3d 680, 700 (N.J. Super. Ct. App. Div. 2013), as the mere fact that some harm follows another act is generally insufficient to show a causal link under New Jersey law, *see Young v. Hobart W. Grp.*, 897 A.2d 1063, 1073–74 (N.J. Super. Ct. App. Div. 2005). Likewise, Rachel Roth does not connect the Ransomware Attack with her information being found on the dark web. *Id.* ¶ 245. Nor does finding her information on the dark web amount to an ascertainable loss. *Thiedemann*, 872 A.2d at 792 ("ascertainable loss" is "either out-of-pocket loss or a demonstration of loss in value").

V. THE COMPLAINT DOES NOT STATE A CLAIM UNDER NEW YORK GBL § 349 (CLAIM 67).

New York GBL § 349 prohibits deceptive acts or practices against the consuming public. *See* N.Y. Gen. Bus. Law § 349(a), (h). To bring a claim for violation of GBL § 349, a plaintiff must plausibly allege three elements: (1) "the challenged act or practice was ***consumer-oriented***"; (2) that the act or practice "was misleading in a material way;" and (3) "the plaintiff suffered injury as a result of the deceptive act." *Stutman v. Chem. Bank*, 731 N.E.2d 608, 611 (N.Y. 2000) (emphasis added). Most importantly, a plaintiff asserting a GBL § 349 claim must adequately plead that the challenged acts and practices are "consumer-oriented." *Maurizio v. Goldsmith*, 230 F.3d 519, 521 (2d Cir. 2000); *S.Q.K.F.C. Inc. v. Bell Atl. Tricon Leasing Corp.*, 84 F.3d 629, 636 (2d Cir. 1996). In other words, a plaintiff must show that the conduct complained of involves a consumer injury or harm to the consuming public at large. *Int'l Sport Divers Ass'n, Inc. v. Marine Midland Bank*, 25 F. Supp. 2d 101, 114 (W.D.N.Y. 1998); *Oswego Laborers' Local 214 Pension*

Fund v. Marine Midland Bank, 647 N.E.2d 741, 744 (N.Y. 1995). For that reason, a claim under GBL § 349 does not follow from a private commercial dispute, only from a consumer-involved transaction. *Citipostal, Inc. v. Unistar Leasing*, 283 A.D.2d 916, 918 (N.Y. App. Div. 2001).

The, New York Plaintiffs do not plausibly allege that Blackbaud has engaged in any consumer-oriented conduct. Rather, the Complaint alleges that Blackbaud provided data security pursuant to a contractual relationship with its clients—business and entities that the Consolidated Complaint calls "Social Good Entities." *See* Compl. ¶¶ 2, 12, 14, 15, 35. Under GBL § 349, then, Blackbaud's contact with its customers—who are not the consuming public—does not give rise to a claim under GBL § 349, which is designed to prohibit deceptive behavior that "ha[s] a broader impact on consumers at large." *Oswego Laborers' Loc. 214 Pension Fund*, 647 N.E.2d at 744. Because "[p]rivate contract disputes, unique to the parties . . . [do] not fall within the ambit of the statute," *id.*, Blackbaud's unique and individualized data storage agreements with its Social-Good-Entity clients are plainly not transactions that GBL § 349 covers.

Nor can Plaintiffs claim some form of indirect injury by Blackbaud's private contractual relationship with its customers. "Although privity between a buyer and seller is not required for a GBL § 349 claim, the buyers must still allege receipt of or exposure to the misleading practice or act." *Szymczak v. Nissan N. Am., Inc.*, No. 10 CV 7493 VB, 2011 WL 7095432, at *15 (S.D.N.Y. Dec. 16, 2011) (citation omitted). Plaintiffs do not allege any exposure whatsoever to Blackbaud's representations about its data security—indeed, neither do the Plaintiffs allege that they were aware of them at all when they entered into their transactions with Blackbaud's clients New Haven Hospital and the Roswell Park Alliance Foundation. Compl. ¶¶ 248-67. Having failed to allege

they had any direct, consumer-based exposure to Blackbaud's services, they cannot now claim the protection of GBL § 349, and these claims fail as a matter of law.[3]

VI. THE COMPLAINT DOES NOT STATE A CAUSE OF ACTION UNDER THE PENNSYLVANIA UTPCPL (CLAIM 75).

Plaintiff Duranko attempts to state a claim under the UTPCPL. To "ensure the fairness of market transactions," *Katz v. Aetna Cas. & Sur. Co.*, 972 F.2d 53, 56 (3d Cir. 1992) (quoting *Pennsylvania v. Monumental Props.*, 329 A.2d 812, 816 (Pa. 1974)), Pennsylvania enacted the UTPCPL, 73 Pa. Stat. § 201-1, *et seq*. Under that statute, "[a]ny person ***who purchases or leases goods or services*** primarily for personal, family or household purposes and thereby ***suffers any ascertainable loss of money or property***, real or personal, as a result of the use or employment by any person of a method, act or practice declared unlawful by section 31 of this act, may bring a private action." *Id.* § 201-9.2 (emphases added).

Accordingly, the UTPCPL has three key pleading requirements that limit its private right of action: a plaintiff must allege (1) she actually purchased or leased goods or services, *id.*; (2) she suffered an "ascertainable loss of money or property" from that purchase or lease transaction, and (3) the loss resulted from the defendant's prohibited conduct under the statute. *Kaymark v. Bank of Am., N.A.*, 783 F.3d 168, 180 (3d Cir. 2015), *abrogated on other grounds by Obduskey v. McCarthy & Holthus LLP*, 139 S. Ct. 1029 (2019). Duranko's allegations satisfy none of those requirements.

[3] Nor may Plaintiffs, as they appear to attempt here, bootstrap a claim relating to New York's data breach laws under GBL § 349. New York's data security law provides only the Attorney General authority to bring suit, N.Y. Gen. Bus. Laws § 899-aa(6)(a), and New York Courts have properly found no private right of action based on the plain text of the statute, *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 19 N.Y.S.3d 850, 857–58 (N.Y. Sup. Ct. 2015). Plaintiffs "cannot circumvent the lack of a private right of action for violation of a New York state law by pleading [their] claim under GBL § 349." *Broder v. Cablevision Sys. Corp.*, 418 F.3d 187, 199 (2nd Cir. 2005); *accord Smahaj v. Retrieval-Masters Creditors Bureau, Inc.*, 131 N.Y.S.3d 817, 827–28 (N.Y. Sup. Ct. 2020).

1. Duranko Fails To Allege That She Is A Purchaser, And She Cannot Allege That She Had Any Business Dealings *With* Blackbaud.

Because the UTPCPL limits claims to plaintiffs who "purchase[ ] or lease[ ] goods or services primarily for personal, family or household purposes," it is unavailable to those who do not make a purchase from, or engage in commercial activity with, the defendant. 73 Pa. Stat. § 201-9.2(a); *accord Balderston v. Medtronic Sofamor Danek, Inc.*, 152 F. Supp. 2d 772, 779 (E.D. Pa. 2001), *aff'd*, 285 F.3d 238 (3d Cir. 2002) (dismissing claim where plaintiff argued only that he was a "purchasing agent" for others).

Here, Duranko does not allege that she purchased or leased any good or service. *See generally* Compl. ¶¶ 309-17. Instead, she alleges that she "provide[d] her [personal health information] to her healthcare provider as a *predicate* to receiving healthcare services." *Id.* ¶ 310 (emphasis added). She does not allege that she consummated the purchase of those healthcare services after providing her information, or even that they were being offered for sale. *See Katz*, 972 F.2d at 55 ("As we have noted, the statute unambiguously permits only persons who have purchased or leased goods or services to sue.").

Furthermore, even if Duranko had properly alleged that she purchased anything, her claim still fails as a matter of law because she does not (and cannot) allege any commercial dealings *with Blackbaud*. "The policy behind the UTPCPL is to place buyers and sellers on equal footing, remedy any unequal bargaining power 'of opposing forces in the marketplace,' and 'ensure fairness of market transactions.'" *Duffy v. Lawyers Title Ins. Co.*, 972 F. Supp. 2d 683, 694 (E.D. Pa. 2013) (quoting *Katz*, 972 F.2d at 55). So, while the UTPCPL does not require direct privity between a plaintiff and defendant, standing to assert a claim does not exist where "a plaintiff lack[s] any commercial dealings with the defendant." *Katz*, 972 F.2d at 57.

Duranko only alleges that she "was required to provide her [personal healthcare information] ***to her healthcare provider*** as a predicate to receiving healthcare services." Compl. ¶ 310 (emphasis added). She then alleges that this information was "in turn provided to Blackbaud to be held for safekeeping." *Id.* But she nowhere asserts that she provided her information to Blackbaud or even that she knew it would be provided to Blackbaud as a part of her dealings with her healthcare provider. *Id.* She does not even allege she was aware that Blackbaud existed or provided any service to her healthcare provider at the time she provided her information. *Id.* In this regard, Duranko simply "did not purchase or lease goods or services from" Blackbaud, did not "otherwise exchange consideration," and was not "the victim[ ] of unequal bargaining power," so the UTPCPL simply does not apply here. *Katz*, 972 F.2d at 56.

Duranko's allegations mirror those in other cases where plaintiffs have unsuccessfully attempted to sue service providers who provided back-end services to the party with whom the plaintiff did business. For example, in *Bessemer System Federal Credit Union v. Fiserv Solutions, LLC*, a credit union brought a UTPCPL claim on behalf of its members, alleging that "it purchase[d] the goods and services at issue, which includes account processing services, online banking capabilities, and ***member information security***, primarily for the personal, family, and household purposes of its members who are individual customers." 472 F. Supp. 3d 142, 179 (W.D. Pa. July 14, 2020) (emphasis added). The court dismissed the claim because the credit union's individual customers lacked the right to sue, since "the misrepresentations at issue were allegedly made only to [the credit union], and there is no allegation that a single [credit union] customer was aware of these representations or in any way relied upon these representations in either choosing to become a [credit union] member or choosing to remain a . . . member." *Id.* The

same is true here—Duranko does not allege any misrepresentation was made *to her* or that she dealt in any way with Blackbaud, and she cannot sustain a UTPCPL claim.

2. Duranko Does Not Allege Any Ascertainable Loss "As A Result Of" Blackbaud's Prohibited Conduct.

Duranko's claim is also insufficient because she fails to allege an ascertainable loss. There can be no claim under the UTPCPL unless the plaintiff alleges that: (1) as a result of her purchase or lease transaction, she justifiably relied upon the defendant's conduct; (2) then suffered "ascertainable loss of money or property, real or personal," 73 Pa. Stat. § 201-9.2(a), which loss must be non-speculative; and (3) the loss was a result of Blackbaud's prohibited conduct under the statute, *Kern v. Lehigh Valley Hosp., Inc.*, 108 A.3d 1281, 1290 (Pa. Super. Ct. 2015); *see also Jarzyna v. Home Props., L.P.*, 185 F. Supp. 3d 612, 626 (E.D. Pa. 2016), *aff'd*, 783 F. App'x 223 (3d Cir. 2019) (speculative damages cannot be an ascertainable loss); *Kaymark*, 783 F.3d at 180.

Initially, Duranko fails to allege ***any*** reliance on Blackbaud's conduct sufficient to sustain her claim. Duranko has not alleged that she was even aware of Blackbaud, let alone aware of any representations it made to her healthcare provider when she provided her healthcare provider her personal information. Absent such allegations, her UTPCPL claim must be dismissed. *Bessemer*, 472 F. Supp. 3d at 179 (dismissing claim where customers did not specifically rely on any representation by their credit union's technology vendor).

Furthermore, none of Duranko's alleged harms are sufficient to state a claim under the UTPCPL. Her alleged lost time, Compl. ¶ 313, without any attendant lost wages, is insufficient to amount to an ascertainable loss under the UTPCPL. *See In re Rutter's Inc. Data Security Breach Litig.*, No. 1:20-CV-382, 2021 WL 29054, at *19 (M.D. Pa. Jan. 5, 2021) (finding only allegations of "lost wages" from time spent on "various remedial actions" sufficient to state a claim). Her alleged emotional distress, Compl. ¶ 315, is "not cognizable" under the UTPCPL. *Walkup v.*

Santander Bank, N.A., 147 F. Supp. 3d 349, 358 (E.D. Pa. 2015) ("Shame, embarrassment, and emotional distress are personal injuries and . . . not cognizable under the UTPCPL."). Her allegation about diminution in the "value" of her personal information, Compl. ¶ 315, is entirely speculative and unquantified, *Riviello v. Chase Bank USA, N.A.*, No. 3:19-CV-0510, 2020 WL 1129956, at *4 (M.D. Pa. Mar. 4, 2020) (damages "cannot be speculative" and must be "identifiable" so unsupported factual allegations are "speculative and unascertainable") (citation omitted); and such damage amounts to a mere "reputational injury," which is not itself a loss of money or property, *Walkup*, 147 F. Supp. 3d at 358. Her vague claim for "violation of privacy" rights, Compl. ¶ 316, might be a "personal injur[y]," *see Walkup*, 147 F. Supp. 3d at 358, but is not a "loss of money or property," as required under this statute, 73 Pa. Stat. § 201-9.2(a). Finally, her claim of future harm from an unspecified identity fraud or future losses of time protecting against that harm, Compl. ¶¶ 315-16, is no more than a precluded, speculative injury. *See Benner v. Bank of Am., N.A.*, 917 F. Supp. 2d 338, 360 (E.D. Pa. 2013) (an outstanding but unpaid fee is not an "ascertainable loss").

VII. THE COMPLAINT DOES NOT STATE A CLAIM UNDER THE SCDBA (CLAIM 79).

The South Carolina Plaintiffs fail to state a claim under the SCDBA on at least two grounds. To state a claim under § 39-1-90, a plaintiff must sufficiently allege the following elements: (1) South Carolina residency, § 39-1-90(G); (2) that the defendant is a "data owner" or "licensor," § 39-1-90(A), and not merely an entity that "maintains" data; and (3) that statutorily-defined "personally identifying information" was involved in the breach, § 39-1-90(A)-(B), (D). To state a claim for damages, plaintiffs must also allege actual damages because of a violation of the statute. § 39-1-90(G)(2). The South Carolina Plaintiffs assert legal conclusions, but they are unable to

point to allege facts that demonstrate that Blackbaud is a data owner or that their personally identifying information was disclosed.

A. Blackbaud Is Not Liable Under South Carolina's Data Breach Security Act Because It Does Not "Own Or License" Data.

Under § 39-1-90(A), only a person "owning or licensing" data is obligated to "disclose a breach . . . to a resident of this State" and must do so "in the most expedient time possible and without unreasonable delay." S.C. Code § 39-1-90(A). A person who merely "maintain[s]" data "shall notify the owner or licensee of the information of a breach of the security of the data." § 39-1-90(B).

Although Plaintiffs allege—in entirely conclusion fashion—that Blackbaud is the owner or licensor of Plaintiff's data, Compl. ¶ 1575, there is no factual support for that allegation. It is a mere naked assertion of a legal conclusion this Court is not required to accept. *ACA Fin. Guar. Corp.*, 917 F.3d at 211. And by the Complaint's other, factual allegations—wherein Plaintiffs acknowledge that Blackbaud "manages, maintains, and provides cloud computing software, services, and cybersecurity for clients including healthcare organizations, education institutions, and other non-profit corporations," Compl. ¶ 419—it is clear that Plaintiffs have alleged only that Blackbaud is a data "maintain[er]" under this statute, S.C. Code Ann. § 39-1-90(B). *See Eagle Container Co., LLC v. Cty. of Newberry*, 666 S.E.2d 892, 896 (S.C. 2008) (courts apply a statute's "plain and unambiguous" meaning). Given the § 39-1-90 distinction between data owners/licensor and data maintainers, with no duty of notice imposed on the latter, § 39-1-90(A)–(B), and the Complaint's lack of factual allegations to support the claim that Blackbaud owed or licensed data, Plaintiffs cannot sustain this claim. *See Morgan v. Haley*, No. 2012-CP-4007331, 2013 WL 8335566, at *2 (S.C. Com. Pl. February 27, 2013) (rote, unsupported allegation that the defendants

were "charged with the duty of securing the personal identifying information" is insufficient under § 39-1-90).

B. There Was No Disclosure Of Personally Identifying Information Triggering the SCDBA.

Even assuming that Blackbaud were an "owner" or "licensor" under § 39-1-90(A) of the SCDBA, an owner or licensor of data is only required to disclose a breach if it involved "personal identifying information." S.C. Code § 39-1-90(A). Personally identifying information is defined as the unencrypted and unredacted "first name or first initial and last name in combination . . . [of] a resident of this State" ***combined with*** any of: (1) a Social Security number; (2) a driver's license number or state identification card number; (3) a financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or (4) any other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual. § 39-1-90(D)(3)(a)-(d).

The South Carolina Plaintiffs have not alleged facts in the Complaint supporting their naked assertion, *see ACA Fin. Guar. Corp.*, 917 F.3d at 211, that that their "personally identifying information," as specifically limited and defined under the statute, was compromised. Ford alleges only that her "name, gender, date of birth, address, date(s) of treatment, department(s) of service, and treating physician(s)" were involved in the Ransomware Attack, which would not meet the definition of § 39-1-90(A). *See* Compl. ¶¶ 322-23. And Scott claims only that his "name, contact information, demographic information, date of birth and [charitable] giving profiles and history" were compromised, which again is insufficient. *Id.* ¶ 333. Critically, the Complaint does not allege that any of the South Carolina Plaintiffs' Social Security numbers, driver's license numbers,

state identification cards, financial account numbers, credit cards, debit cards, or other numbers or information specifically delineated under the statute were impacted by the Ransomware Attack. *See* S.C. Code § 39-1-90(D)(3)(a)-(d). Since the South Carolina Plaintiffs' names were not impacted "in combination with" a statutorily-listed "data element[ ]," Plaintiffs have failed to state a claim under § 39-1-90(A).

CONCLUSION

For the foregoing reasons, the statutory claims within the Consolidated Class Action Complaint should be dismissed with prejudice for failure to state a claim upon which relief may be granted.